

Konfiguration des Access Points Zyxel ZyAir G-1000 54 Mbps

Weitere Komponenten, die Sie im Netzwerk benötigen, sind ein oder mehrere Access Points. Im folgenden Dokument wird die Konfiguration eines Zyxel ZyAir G-1000 Access Points beschrieben.

Wenn Sie den Router wie im Dokument *Konfiguration der Netzwerkeinstellungen und des DHCP-Dienstes* eingestellt haben, können Sie nun den Access Point (AP) anhand der Zeichnung in das Netzwerk einbinden (Zeichnung, Abb. 1).

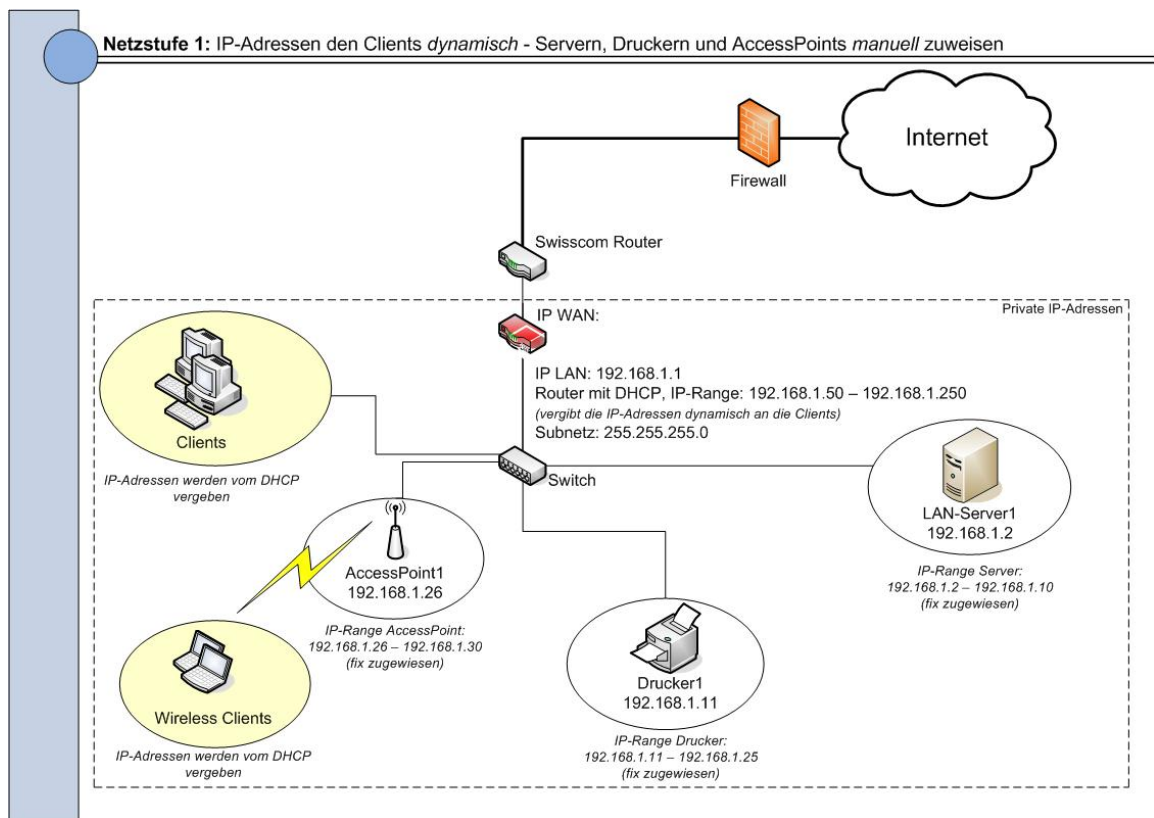


Abb. 1

1. Vorbereitung

Um den AP zu konfigurieren muss der Client mit diesem kommunizieren können. Deshalb müssen Sie dem Client zuerst das drahtlose Netzwerk des AP „zeigen“. Dazu machen Sie einen Rechtsklick auf *Netzwerkumgebung* -> *Eigenschaften* und öffnen durch einen wiederholten Rechtsklick auf *Drahtlose Netzwerkverbindung* -> *Verfügbare drahtlose Netzwerke anzeigen* folgendes Fenster (siehe Abb. 2).

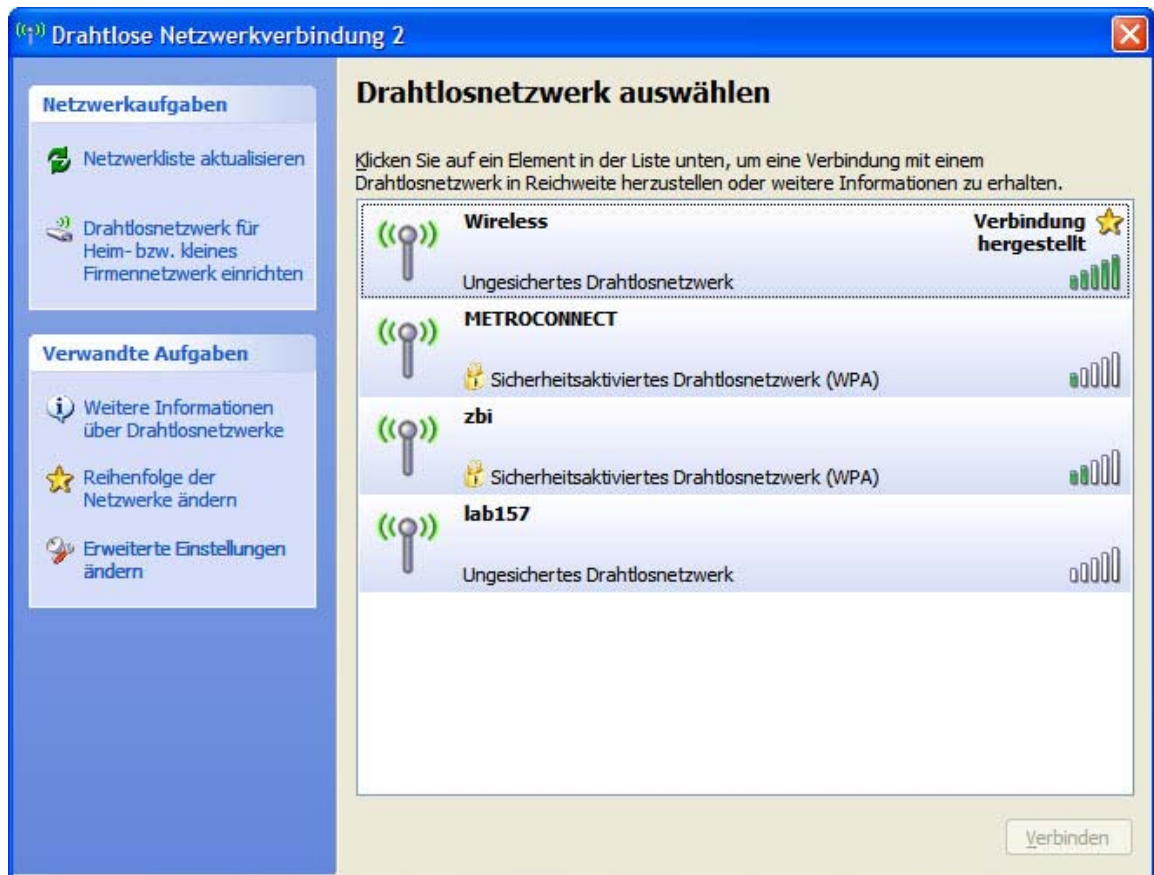


Abb. 2

Der AP meldet sich mit dem Standardnamen „Wireless“. Wählen Sie nun diese drahtlose Verbindung aus und klicken auf „Verbinden“.

Starten Sie den Browser. Geben Sie im Browser die IP-Adresse des AP (192.168.1.2) ein.
(Falls Sie bei der Internetverbindung einen Proxy verwenden, sollten Sie zur Konfiguration des AP den Proxy deaktivieren. Dies können Sie in den Optionen Ihres Browsers tun).

Nach der Änderung des Passwortes erfolgt die eigentliche Konfiguration des Access Points.
Klicken Sie einfach auf „Wizard Setup“ um die entsprechenden Einstellungen vorzunehmen.

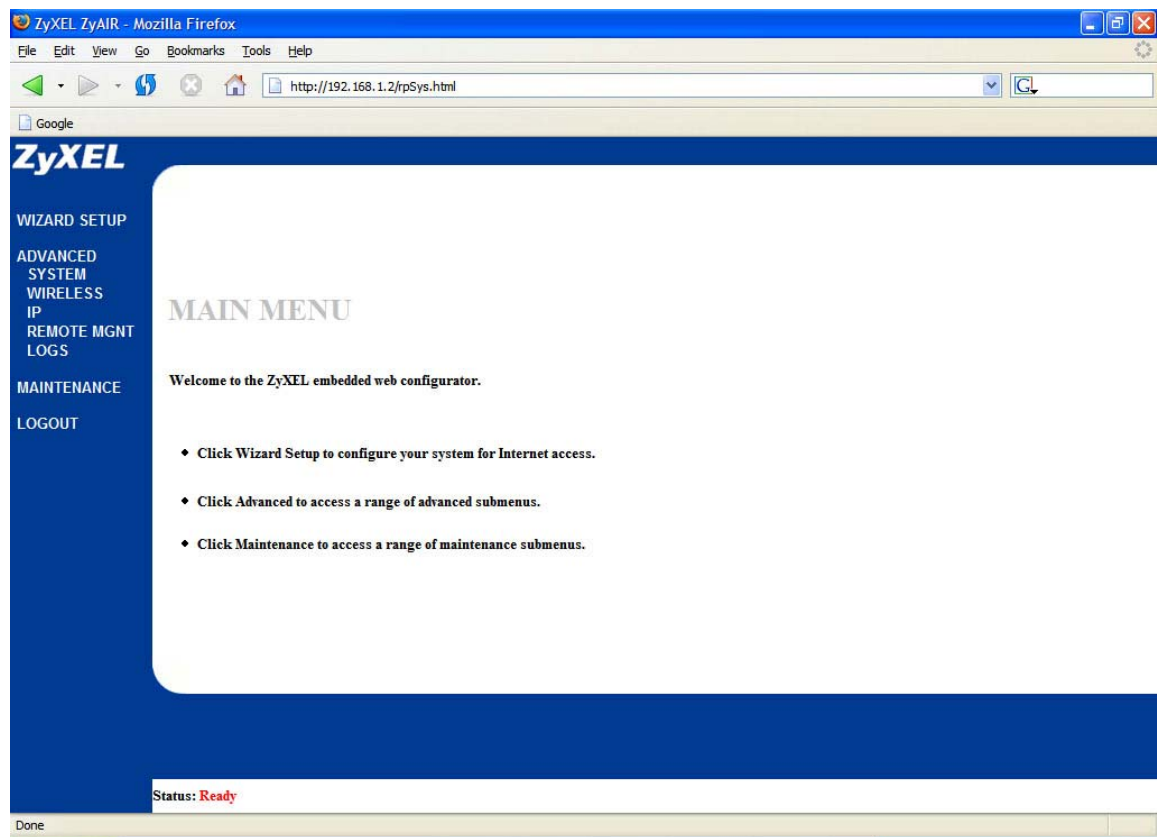


Abb. 3

2. Wizard Setup - Grundeinstellungen

Als erstes geben Sie dem AP einen eindeutigen Namen. Dieser wird dann im Intranet zu sehen sein. Den *Domain Name* können Sie leer lassen.

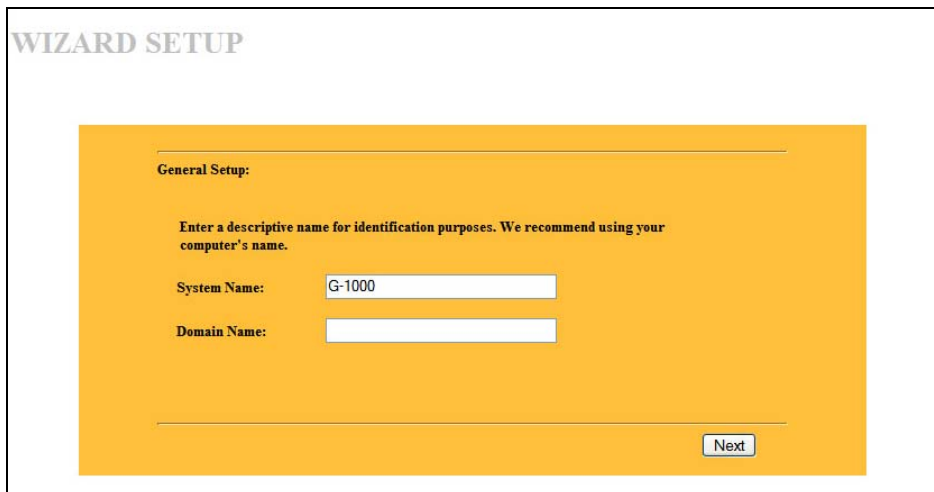


Abb. 4

Als nächstes müssen Sie dem ZyAIR eine ESSID vergeben. Diese ist nötig, um den AP im Drahtlosnetzwerk eindeutig zu identifizieren. Ausserdem müssen Sie unter „Choose Channel ID“ die gewünschte Frequenz wählen, über welche kommuniziert werden soll. Die Frequenz können Sie frei wählen. Jeder AP muss auf einer eigenen Frequenz arbeiten. Natürlich wird die Verbindung verschlüsselt, damit unbefugte Personen keinen Zugriff darauf haben. Die Verschlüsselung machen wir jedoch nicht mit WEP, weil dies zu unsicher ist. Deshalb setzen wir „WEP Encryption“ auf *Disable* (siehe Abb. 5), da wir die Verschlüsselung mit Hilfe der WPA-Methode empfehlen.

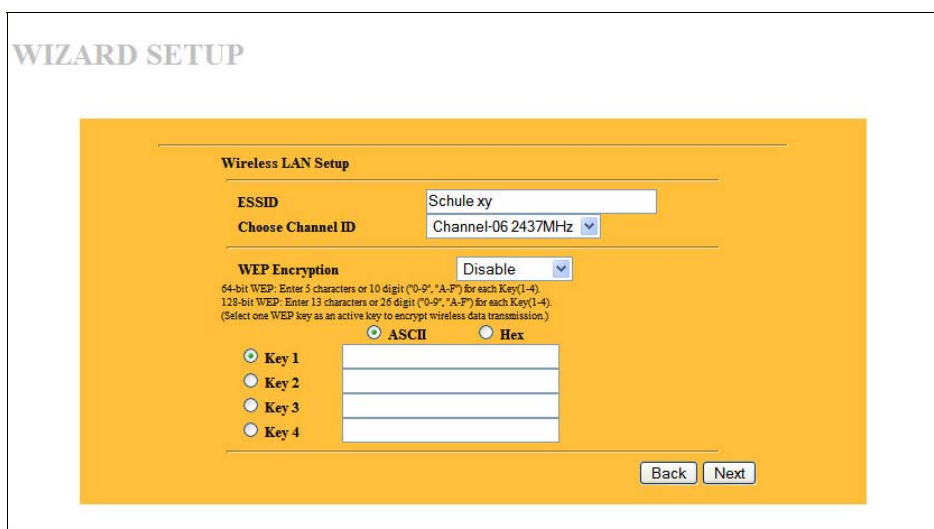


Abb. 5

Unter 3.1 wird die Verschlüsselung per WPA vorgeschlagen. Dies ist aber nur möglich, wenn Soft- und Hardware entsprechende Voraussetzungen haben.

Der letzte Punkt im Wizard Setup ist die IP-Adresse des Access Points. Wie auf der Zeichnung (Abb. 1) zu sehen ist, hat es einen vorgegebenen IP-Range für die Access Points. Da dies der erste AP im Netzwerk ist, hat er die IP-Adresse 192.168.1.26. Die restlichen Angaben (Subnetzmaske und Gateway) sind von der Zeichnung zu entnehmen.

WIZARD SETUP

IP Address Assignment

☐ Get automatically from DHCP

☒ Use fixed IP address

IP Address	192.168.1.26
IP Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.1

Back Finish

Abb. 6

3. Advanced Setup – Erweiterte Konfiguration

3.1 WPA - Verschlüsselung

Die Basiskonfiguration ist nun abgeschlossen. Wie vorher schon erwähnt ist es wichtig, eine verschlüsselte Verbindung herzustellen. Dazu verwenden wir die so genannte WPA - Verschlüsselung (Wi-Fi Protected Access). Diese ist sehr viel sicherer als die WEP - Verschlüsselungsart. Um die WPA-Verschlüsselung zu aktivieren, gehen Sie im Menu Advanced unter Wireless und wählen dort die Karteikarte *802.1x/WPA*. Bei *Wireless Port Control* wählen sie „Authentication Required“ aus und nehmen die Einstellungen gem. Abb. 7 vor.

Wichtig: Die Voraussetzung für eine WPA-Verschlüsselung ist Windows XP mit Service Pack 2. Bei älteren Versionen von Windows (inbegriffen SP1), müssen gewisse Anpassungen im System vorgenommen werden, die Sie unter folgendem Link finden:
(<http://www.microsoft.com/germany/technet/datenbank/articles/600207.msp#E4E>).

Bei *Pre-Shared Key* müssen Sie einen Key eingeben, ähnlich wie ein Passwort. Bei jedem Verbindungsaufbau muss dieser dann eingegeben werden. Unbefugte Personen können ohne den Key nicht auf die Wireless-Verbindung zugreifen.

The screenshot shows the 'WIRELESS LAN' configuration window with the '802.1X/WPA' tab selected. The settings are as follows:

Section	Setting	Value	Unit/Note
802.1X Authentication	Wireless Port Control	Authentication Required	Dropdown menu
	ReAuthentication Timer	1800	(In Seconds)
	Idle Timeout	3600	(In Seconds)
Key Management Protocol	Key Management Protocol	WPA-PSK	Dropdown menu
	Pre-Shared Key	2006bernsai	Text field
	WPA Mixed Mode	Disable	Dropdown menu
	WPA Group Key Update Timer	1800	(seconds)

Buttons: Apply, Reset

Abb. 7

Wenn die WPA-Verschlüsselung geklappt hat, sollte jetzt bei den Wireless Netzwerken (Rechtsklick auf Netzwerkumgebung -> Eigenschaften -> Rechtsklick auf Drahtlose Netzwerkverbindung -> Verfügbare drahtlose Netzwerke anzeigen) folgendes zu sehen sein: (Abb. 8, Nr. 1)

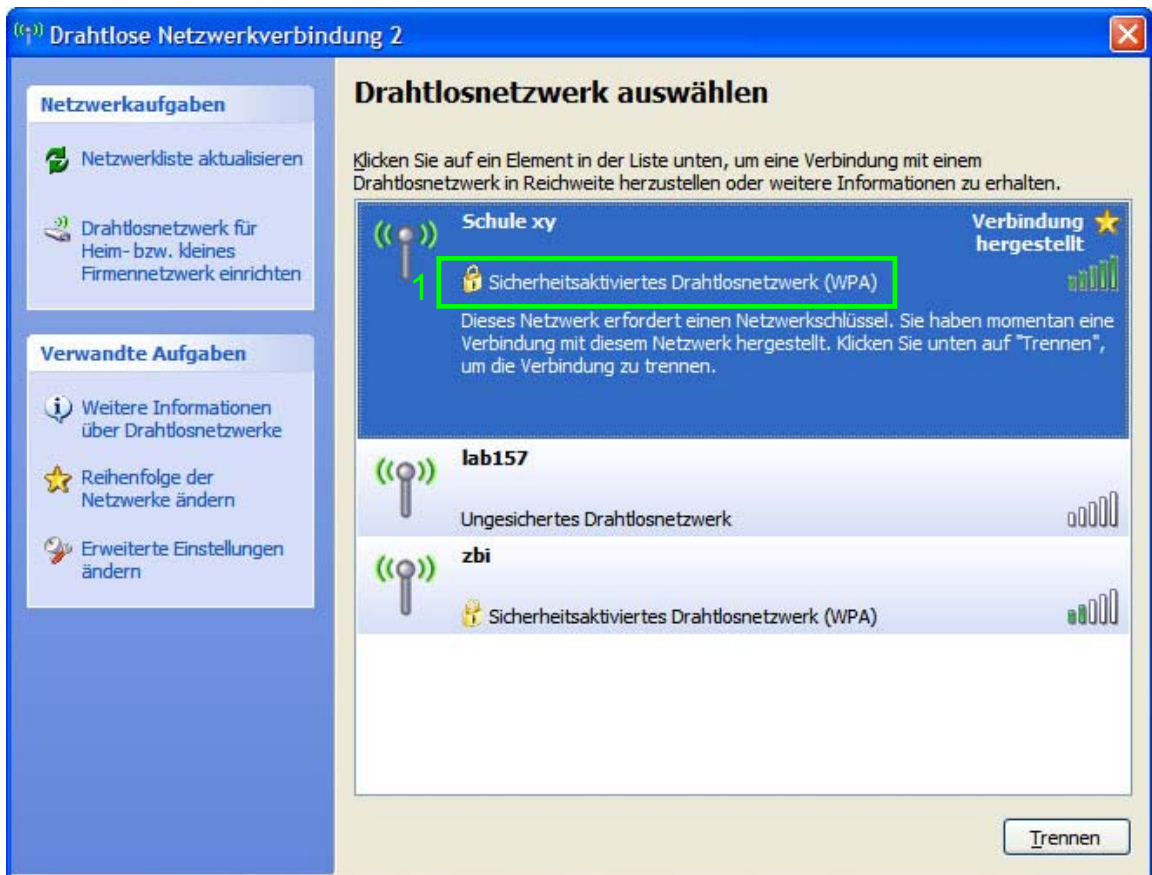


Abb. 8

3.2 Roaming

Wenn sich in Ihrem Netzwerk mehr als ein Access Point befinden, empfehlen wir Ihnen das so genannte „Roaming“ einzusetzen. So ist es den Clients möglich, problemlos zwischen den Access Points zu wechseln, ohne einmal die Verbindung zu unterbrechen. Der Client wählt den AP aus, von dem er das stärkste Signal empfängt.

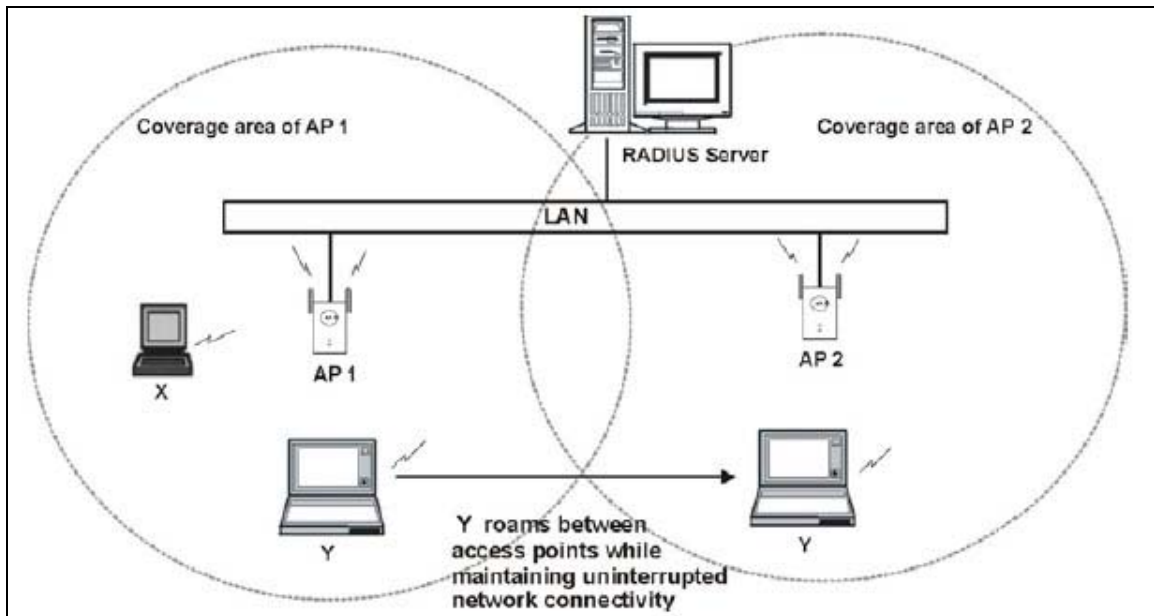


Abb. 9

Um das Roaming beim Access Point zu aktivieren, müssen Sie unter *Advanced -> Wireless -> Roaming* „Active“ auf Yes setzen. Der standardmäßige Port ist 16290.

Wichtig ist, dass alle Access Points im Subnetz die gleiche ESSID haben, sonst funktioniert Roaming nicht!

WIRELESS LAN

Wireless	MAC Filter	Roaming	802.1x/WPA	Local User Database	RADIUS
Roaming Configuration					
Active		Yes <input type="button" value="v"/>			
Port		16290			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

Abb. 10